"The City of Heritage"

ULUNDI
MUNICIPALITY

INFORMATION TECHNOLOGY

Backup and Restore Policy

Table of Contents

1. Overview

This policy defines the backup policy for computers within the municipality which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, Pastel.

2. Purpose

All electronic information considered of municipal value should be copied onto secure storage media on a regular basis (i.e., backed up), for disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs, identified through technical risk analysis that exceeds these requirements, should be accommodated on an individual basis.

3. Scope

Data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. Backup provisions allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of municipal data backups need to be maintained.

4. Definitions

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

Municipality Critical Data - Data that if it were deemed unavailable to the Municipality will have an immediate (within 24 hours) critical impact on the Municipality.

Data Owners - Department managers, members of the top management team, or their delegates who bear responsibility for the acquisition, development, and maintenance of production applications that process Municipality information

Data Custodians - Are in physical or logical possession of either Municipality information or information that has been entrusted to them. Ulundi Municipality Custodians are responsible for safeguarding the information and making backups so that critical information is not lost.

FTP – (File Transfer Protocol) - Data is transferred from one department/computer to another over the internet.

5. System Backups

5.1 Payday Backups

- Manual Backup
  - PAYDAY operator runs backups once a week.
  - Data is stored daily in PAYDAY folder on the File Server.
- Off-site Storage
  - PAYDAY consultant takes an off-site backup monthly.

5.2 Pastel

- Manual Backup
  - Pastel Evolution (files and folders) daily backups are stored on the Pastel Server;
- Off-site Storage
  - PAYDAY consultant takes an off-site backup once a week.
- On-Line Backup
  - Pastel monthly online backups stored onto our Backup System.

5.3. File Server

- Automatic Backup
  - Backup runs automatically at 22h00 on weekdays.
  - The file server backup system is set to backup all critical data that has been stored on the server:
  - PAYDAY,
  - Metval,
  - Finance Folder;
  - Data Files
- Pastel Evolution and any other critical data.
  - The data is copied to disk or external device for external storage, weekly.
  - The data from the File Server is also backed up to our Backup system, monthly.

6. Data Backed Up

i) Data to be backed up has to include the following information:
   a. User data stored on the local hard drive and File Server;
   b. System Databases; and

c. System Configurations.

ii) Systems to be backed up has to include but are not limited to:

a. File server;

b. Production database server; and

c. Domain controllers (Active Directory).

7. Testing

The ability to restore data from backups shall be tested at least once every six months. Business Vendors will also be required to perform backup testing as per the agreed upon SLAs

7.1. Restoration of Back-ups

On a monthly basis a restoration of one back-up from each system must be performed to ensure that back-ups can be restored in an effective and timely manner. The restoration must be performed on a test environment to ensure that it does not impact on the production environment. Documented evidence of the back-up restorations must be retained. The restore process should be recorded accordingly on the “Backup Recovery Testing Log” (see Appendix C).

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

8. Retention Period

The following retention periods are applicable for all types of back-up:

- Daily – Backup will be retained for a week on the File server;
- Weekly – Backup will be retained for 4 weeks;
- Monthly – Backup will be retained for 12 months; and

Retention periods for backup information should be determined, with ideally at least 5 complete backup cycles in place prior to disposal or deletion.

9. Operator Logs

- The IT Department will maintain an activity log and system reports for each system they are responsible for. This will include:

- System start/finish times, for planned downtime, unplanned downtime and system maintenance routines;
- System error reports and corrective action taken; and
- Operator identification for each log entry.

10. Responsibility

The IT Manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a quarterly basis. Backup reports must be generated and a Backup Register must also be kept with reference to backup status.

11. Archives

User account data associated with the file are archived one month after they have left the municipality. Pastel and PAYDAY Systems are not archived as it is not deemed necessary.

12. Backup Media Storage Locations

Offline Backup server used for daily backups shall be stored on-site office. Offsite storage is at Protection Department (Licensing) about 2km away.

13. Approvals

The table below provides necessary approvals of this policy.

Approver	**Signature**	**Date**
Chairman of the Council		
Chairman of the Audit and Risk Committee		
Ulundi Municipal Manager		